

21197

#2



IN THE U.S. PATENT AND TRADEMARK OFFICE

Inventor Massimo BALESTRI et al
Patent App. Not known
Filed Concurrently herewith
For METHOD AND SYSTEM FOR THE CONTROLLED DELIVERY
 OF DIGITAL SERVICES, SUCH AS MULTIMEDIA
 TELEMATICS SERVICES

Art Unit Not known

Hon. Commissioner of Patents
Washington, DC 20231


TRANSMITTAL OF PRIORITY PAPERS

In support of the claim for priority under 35 USC 119,
Applicant herewith encloses a certified copy of each application
listed below:

<u>Number</u>	<u>Filing date</u>	<u>Country</u>
TO98A000705	11 August 1998	Italy.

Please acknowledge receipt of the above-listed documents.

Respectfully submitted,
The Firm of Karl F. Ross P.C.


by: Andrew Wilford, 26,597
Attorney for Applicant

14 July 1999
5676 Riverdale Avenue Box 900
Riverdale (Bronx), NY 10471-0900
Cust. No.: 000535
Tel: (718) 884-6600
Fax: (718) 601-1099
je

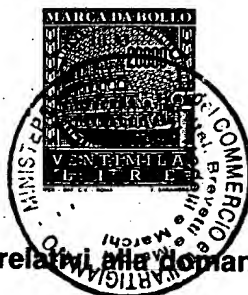
21197

MODULARIO
I.C.A. - 101

Mod. C.E. - 1-4-7



MINISTERO DELL'INDUSTRIA, DEL COMMERCIO E DELL'ARTIGIANATO
DIREZIONE GENERALE DELLA PRODUZIONE INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI



10530 U.S. PRO
09/354080
07/18/99

INV. IND.

Autenticazione di copia di documenti relativi alla domanda di brevetto per

N.T098 A-000705

*Si dichiara che l'unita copia è conforme ai documenti originali
depositati con la domanda di brevetto sopraspecificata, i cui dati
risultano dall'accluso processo verbale di deposito*

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

15 GIU. 1999

IL REGGENTE

IL DIRETTORE DELLA DIVISIONE

D.ssa Paola DI CINTIO

Paola Di Cintio



A. RICHIEDENTE (I)

1) Denominazione **CSELT CENTRO STUDI E LABORATORI TELECOMUNICAZIONI S.P.A.**
 Residenza **TORINO** **TO** codice **00527770010**

2) Denominazione _____
 Residenza _____ codice _____

B. RAPPRESENTANTE DEL RICHIEDENTE PRESSO L'U.I.B.M.

cognome e nome **vs. Paolo CERNI** ed altri. cod. fiscale _____
 denominazione studio di appartenenza **JACOBACCI & PERANI S.p.A.**
 via **Corso Regio Parco** n. **27** città **TORINO** cap **10152** (prov) **TO**

C. DOMICILIO ELETTIVO destinatario

via _____ n. _____ città _____ cap _____ (prov) _____

D. TITOLO

classe proposta (sez/cl/sci) _____

gruppo/sottogruppo _____

**PROCEDIMENTO E SISTEMA PER L'EROGAZIONE CONTROLLATA DI SERVIZI
 NUMERICI QUALI, AD ESEMPIO, SERVIZI TELEMATICI MULTIMEDIALI**

ANTICIPATA ACCESSIBILITÀ AL PUBBLICO: SI ☐ NO ☒

SE ISTANZA: DATA _____ N° PROTOCOLLO _____

E. INVENTORI DESIGNATI

cognome nome

cognome nome

1) **BALESTRI MASSIMO** 3) _____
 2) **DE PETRIS GIANLUCA** 4) _____

F. PRIORITÀ

nazione o organizzazione	tipo di priorità	numero di domanda	data di deposito	allegato S/R	SCIOGLIMENTO RISERVE Data N° Protocollo
1) _____	_____	_____	____/____/____	_____	____/____/____
2) _____	_____	_____	____/____/____	_____	____/____/____

G. CENTRO ABILITATO DI RACCOLTA COLTURE DI MICRORGANISMI, denominazione

H. ANNOTAZIONI SPECIALI

DOCUMENTAZIONE ALLEGATA

N. es.

Doc.	N. es.	Prov.	n. pag.	n. tav.	Descrizione	SCIOGLIMENTO RISERVE Data N° Protocollo
Doc. 1)	2	PROV.	27		riassunto con disegno principale, descrizione e rivendicazioni (obbligatorio 1 esemplare)	____/____/____
Doc. 2)	2	PROV.		02	disegno (obbligatorio se citato in descrizione, 1 esemplare	____/____/____
Doc. 3)	1	RIS.			lettera d'incarico, procura o riferimento procura generale	____/____/____
Doc. 4)	0	RIS.			designazione inventore	____/____/____
Doc. 5)	0	RIS.			documenti di priorità con traduzione in italiano	____/____/____
Doc. 6)	0	RIS.			autorizzazione o atto di cessione	____/____/____
Doc. 7)	0				nominativo completo del richiedente	____/____/____

8) attestati di versamento, totale lire **CINQUECENTO SESSANTACINQUEMILA..=** obbligatorioCOMPILATO IL **11 08 1998** FIRMA DEL (I) RICHIEDENTE (I) _____CONTINUA SINO **NO**DEL PRESENTE ATTO SI RICHIEDE COPIA AUTENTICA SINO **SI****JACOBACCI & PERANI S.p.A.**

UFFICIO PROVINCIALE IND. COMM. ART. DI

TORINO

VERBALE DI DEPOSITO NUMERO DI DOMANDA

Reg. A

L'anno millenovecento **Novantotto** **TO 98A 000705**, del mese di **Agosto**Il (I) richiedente (I) sopraindicato (I) ha (hanno) presentato a me sottoscritto la presente domanda, corredate di n. **01** allegativi per la concessione del brevetto soprariportato.

I. ANNOTAZIONI VARIE DELL'UFFICIO ROGANTE

IL DEPOSITANTE

DINO CHIALE

L'UFFICIALE ROGANTE

V. QUALIFICA E INIZIALE

NUMERO DOMANDA

NUMERO BREVETTO

A. RICHIEDENTE (I)

Denominazione

Residenza

CSELT CENTRO STUDI E LABORATORI
TORINO

BEG. A

DATA DI DEPOSITO

DATA DI RILASCIO

11/08/1998

TELECOMUNICAZIONI S.P.A.

D. TITOLO

PROCEDIMENTO E SISTEMA PER L'EROGAZIONE CONTROLLATA DI SERVIZI
NUMERICI QUALI, AD ESEMPIO, SERVIZI TELEMATICI MULTIMEDIALI

Classe proposta (sez./cl./scl/)

(gruppo/sottogruppo)

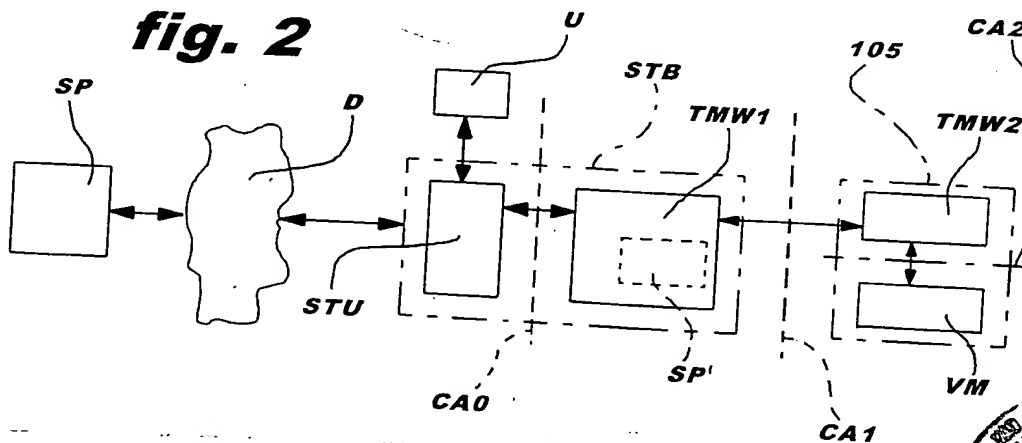
L. RIASSUNTO

I servizi erogati da una pluralità di fornitori (SP) verso gli utenti (U) sono identificati da rispettivi flussi di dati codificati, ad esempio di tipo MPEG. Gli utenti (U) sono provvisti di rispettivi mezzi di ricezione (STB) di tipo generalizzato, comune a tutti gli utenti. Ciascun utente è provvisto di un'unità di utente (105), realizzata di preferenza sotto forma di una smart card, incorporante una funzione elaborativa (VM) suscettibile di riconoscere, caricare ed eseguire almeno un algoritmo di abilitazione incorporato nei flussi di dati inviati dai fornitori sulla base di un rispettivo codice identificativo, anch'esso incorporato nei flussi di dati erogati, per abilitare i mezzi di ricezione, attraverso l'unità di utente (105), alla fruizione del rispettivo servizio. (Figura 2)



M. DISEGNO

fig. 2



DESCRIZIONE dell'invenzione industriale dal titolo:
"Procedimento e sistema per l'erogazione controllata
di servizi numerici quali, ad esempio, servizi tele-
matici multimediali"

di: CSELT - Centro Studi e Laboratori Telecomunica-
zioni S.p.A., nazionalità italiana, Via G. Reiss Ro-
moli, 274 - Torino

Inventori designati: Massimo BALESTRI, Gianluca DE
PETRIS

Depositata il: 11 agosto 1998

TO 98A 000705

* * *

TESTO DELLA DESCRIZIONE

La presente invenzione si riferisce all'eroga-
zione controllata di servizi numerici quali, ad
esempio, servizi telematici multimediali, ed è stata
sviluppata con particolare attenzione alla possibile
applicazione nell'ambito della cosiddetta iniziativa
OPIMA (Open Platform Initiative for Multimedia Ac-
cess).

Una descrizione delle finalità e dei criteri
che regolano tale iniziativa è accessibile alla data
di deposito della presente domanda sul sito Internet
<http://www.cselt.it/ufv/leonardo/opima>.

Ulteriori informazioni di contesto sono desumi-
bili ad esempio dalla norma CENELEC EN 50221, deno-

LB/mtr



minata "DVB Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications" o ancora nel documento DAVIC 1.3 Part 10: "Basic Security Tools for Davic 1.3", pubblicato nel novembre 1997 su CD-Rom disponibile presso la Segreteria DAVIC c/o Società Italiana Avionica S.p.A., Strada Antica di Collegno, 235; I-10146 Torino.

L'invenzione è però suscettibile di trovare applicazione in tutte quelle situazioni in cui si desidera realizzare un sistema tale da consentire ad un utilizzatore o utente di avere accesso, con un unico decodificatore, ad informazioni codificate di fornitori (provider) diversi. L'invenzione può quindi trovare impiego in servizi diffusivi via satellite o cavo di tipo numerico, ad esempio per la fornitura di contenuti audiovisivi a pagamento, anche di tipo interattivo. Un sistema secondo l'invenzione può essere realizzato all'interno di un decodificatore del tipo correntemente denominato Set Top Box (STB), nell'ambito di un personal computer, oppure integrato direttamente, ad esempio, in un ricevitore quale un ricevitore televisivo con interfaccia di tipo numerico.

In questo contesto sono già state proposte e

sperimentate soluzioni in cui l'accesso alle informazioni (tipicamente un programma televisivo) presuppone la disponibilità, presso l'utente, di un dispositivo decodificatore, essenzialmente di tipo proprietario del fornitore del servizio. In altre parole, un determinato dispositivo decodificatore consente di ricevere soltanto i programmi trasmessi da un certo fornitore di servizi o, al più, da un ristretto numero di fornitori che adottano le stesse modalità di erogazione dei servizi.

In generale, per poter accedere a fornitori diversi, l'utilizzatore è però costretto a provvedersi di una molteplicità di dispositivi diversi, usando alternativamente ora l'uno, ora l'altro dispositivo.

Tentativi di conseguire un certo grado di standardizzazione sono già stati compiuti ad esempio con la definizione, da parte del Forum Internazionale DAVIC, della cosiddetta interfaccia CA0 e, soprattutto, con la definizione della cosiddetta interfaccia CA1, illustrata in dettaglio nel documento DAVIC 1.3 già citato in precedenza.

In sostanza, le suddette due interfacce operano ai due livelli indicati rispettivamente con linee a tratto e punto nello schema della figura 1, destinato ad essere utilizzato per illustrare tanto le so-

luzioni secondo la tecnica nota quanto la soluzione secondo l'invenzione.

In tale schema i riferimenti SP ed U indicano, rispettivamente, un fornitore (provider) di servizi informativi ed un utilizzatore o utente degli stessi.

Tali servizi possono essere servizi informativi diversi, quali (ma senza limitazione a): programmi audio e/o televisivi, in particolare erogati secondo modalità di richiesta e pagamento diversi, servizi a valore aggiunto, servizi pubblicitari, anche a premio, servizi in abbonamento o erogati sulla base di buoni (coupon), servizi informativi vari (bancari e di borsa, sul traffico, di localizzazione, ecc.), giochi, distribuzione di software, televendite, servizi bancari a distanza, servizi di rilevazione demoscopica, anche di tipo interattivo.

Sempre nello schema della figura 1 il riferimento D indica il mezzo (diffusione via cavo, via satellite, terrestre, in rete dedicata, su Internet, ecc.) attraverso il quale l'informazione generata dal fornitore SP perviene al sistema di ricezione STB dell'utilizzatore U.

Nello standard DAVIC 1.3 già citato in precedenza, tale informazione è presente sotto forma di



un flusso dati MPEG (acronimo per Moving Picture Expert Group), in particolare come un flusso codificato secondo le relative normative ISO/IEC 13818 (MPEG-2). In tale flusso vengono inseriti messaggi noti rispettivamente come ECM ed EMM. L'acronimo ECM, che sta per Entitlement Control Message, identifica i messaggi di controllo associati ad un servizio. L'acronimo EMM, che sta per Entitlement Management Message, identifica invece i messaggi di gestione delle autorizzazioni alla fruizione di servizi associati ad un utente.

Nell'unità STU (ovverosia Set Top Unit, che insieme al blocco di sicurezza indicato complessivamente con SD costituisce il sistema di ricezione STB a disposizione dell'utente U) è presentato in primo luogo un blocco ricevitore 100 destinato a realizzare la ricezione a livello hardware (demodulazione, sincronizzazione, ecc.) del flusso dati in ingresso. Quest'ultimo è destinato ad essere inviato verso il blocco SD ed in particolare verso un filtro 101 ed un blocco di decifrazione o decriptazione 102.

I segnali inviati secondo lo standard MPEG possono essere crittografati così da consentirne la lettura in chiaro soltanto dagli utilizzatori abilitati con un'opportuna chiave.

La funzione di decriptazione è pilotata, nell'ambito dell'unità STU, dal modulo di gestione 103 che invia tramite una rispettiva interfaccia di comando istruzioni verso un modulo 104. Quest'ultimo funge, nell'ambito del blocco SD, da elemento di gestione della sicurezza (cosiddetto Security Manager). In pratica, la funzione del modulo 104 è quella di interagire con il filtro 101, con il modulo di decifrazione o decriptazione 102 e con un'unità di utente 105 per fornire verso il modulo 102 una chiave di decifrazione tale da consentire al modulo 102 stesso di decifrare il segnale in arrivo dal ricevitore 100. Questo segnale può così essere reso in chiaro e trasferito a un demultiplicatore 106 e ad un decodificatore 107 (ovvero ad una catena di elaborazione equivalente) contenuti nell'unità STU in vista dell'erogazione verso l'utente U.

Nei sistemi più tradizionali a cui si è fatto cenno in precedenza (del tipo di quelli che implementano la cosiddetta interfaccia CAO nella terminologia corrente in ambito DAVIC) la standardizzazione del sistema di ricezione STB in funzione dei vari fornitori dei servizi SP si limita alla sola unità STU.

Tutto quanto sta al disotto della linea a trat-

to e punto che nella figura 1 identifica l'interfaccia CA0 costituisce una parte di dispositivo specializzato in funzione di un determinato fornitore di servizi.

L'adozione dell'interfaccia CA1 consente di standardizzare anche l'unità SD, spostando l'esigenza di specializzazione ad un livello più basso, ossia a quello dell'unità di utente 105 per la quale è prevista la realizzazione in forma amovibile, in particolare sotto forma di una cosiddetta "smart card".

Tuttavia, anche ricorrendo alla realizzazione come smart card, i problemi delineati in precedenza non vengono comunque risolti ma semplicemente trasferiti ad un livello diverso.

L'utente o utilizzatore che desideri ricevere l'informazione da fornitori SP diversi dovrà in generale munirsi di tante unità di utente 105, dunque di tante smart card diverse, una per ciascun fornitore.

Oltre a doversi provvedere di più smart card, l'utente dovrebbe comunque di volta in volta riconfigurare il suo sistema di ricezione in funzione del fornitore dei servizi che si desiderano ricevere, ad esempio inserendo nel sistema la smart card corri-

spondente.

La scarsa praticità di questo modo di operare è evidente, soprattutto se si tiene conto del fatto che in uno scenario del tipo di quello dell'iniziativa OPIMA si desidera fornire all'utente modalità di selezione dei fornitori SP sostanzialmente analoghe a quelle normalmente adottate nella ricezione dei programmi televisivi: in pratica la possibilità di scegliere fornitore e servizio tramite una semplice azione esercitata su un telecomando.

Almeno in linea di principio gli inconvenienti sopra delineati potrebbero essere risolti prevedendo l'inserimento di più unità di utente 105 nel sistema di ricezione.

Anche in modo indipendente da ogni considerazione sulla complessità del sistema, questa soluzione non risolverebbe comunque il problema legato all'esigenza, per l'utente, di munirsi di più unità di utente 105.

La presente invenzione si prefigge lo scopo di fornire una soluzione in grado di evitare gli inconvenienti delineati in precedenza, in particolare in relazione alla possibile adozione delle interfacce definite come CA0 e CA1, pur conservando generali doti di conformità con tali interfacce.



Secondo la presente invenzione, tale scopo viene raggiunto grazie ad un procedimento per l'erogazione di servizi avente le caratteristiche richiamate in modo specifico nelle rivendicazioni che seguono. L'invenzione ha anche per oggetto il relativo sistema.

L'invenzione verrà ora descritta, a puro titolo di esempio non limitativo, con riferimento ai disegni annessi, nei quali:

- la figura 1, rappresentativa - in termini generali - anche delle soluzioni secondo la tecnica nota, è già stata esaminata in precedenza,

- la figura 2 illustra, sotto forma di uno schema a blocchi funzionale corrispondente al modello di riferimento OPIMA (OPIMA Reference Model) una possibile forma di attuazione dell'invenzione, e

- la figura 3 illustra, sotto forma di un diagramma di flusso, una possibile sequenza di funzionamento di un sistema secondo l'invenzione.

Nella figura 2 elementi identici o corrispondenti a quelli già descritti con riferimento alla figura 1 sono stati indicati con gli stessi riferimenti che già appaiono nella figura 1.

Ciò vale in particolare per il fornitore dei servizi SP, il canale di distribuzione D verso l'u-

tente U, l'unità STU e l'ideale collocazione delle interfacce CA0 e CA1.

Il complesso delle funzioni illustrate con riferimento alla figura 1 facendo riferimento ai moduli 101, 102, 104 è svolto, nello schema secondo l'invenzione della figura 2, da un complesso di elementi rappresentato dai blocchi TMW1, TMW2 e VM. La sigla TMW utilizzata per entrambi i blocchi TMW1 e TMW2 sta ad indicare il fatto che tali blocchi vengono normalmente realizzati a livello di cosiddetto "trusted middleware" (ossia di software che realizza funzioni di sicurezza).

In sintesi, la soluzione secondo l'invenzione può essere vista come uno sviluppo della soluzione basata sull'interfaccia CA1. Nella soluzione secondo l'invenzione la smart card 105 oltre a contenere una chiave crittografica non modificabile né leggibile dall'esterno, è in grado di ricevere, verificare, immagazzinare ed eseguire un algoritmo che consente la fruizione dei servizi erogati da un determinato fornitore.

La fase di verifica mira a provare l'autenticità e l'integrità dell'algoritmo prima che venga immagazzinato nella smart card, ed è basata sul controllo di una firma crittografata digitale eseguita

da una Autorità di Certificazione riconosciuta dai fornitori dei servizi e dai produttori delle smart card.

L'esecuzione dell'algoritmo specifico del fornitore di servizi permette di decifrare i messaggi EMM/ECM proprietari del fornitore di servizi stesso e di alimentare il modulo di decifrazione 102 che provvede a mettere in chiaro i servizi richiesti dall'utente, consentendone.

In questo modo l'utente non ha più necessità di provvedersi di più unità 105 per poter ricevere informazioni da fornitori diversi.

Secondo l'invenzione è infatti sufficiente disporre, ad esempio, di un'unica smart card, di tipo universale, e le informazioni relative alla specializzazione, necessarie per poter ricevere in chiaro le informazioni di un determinato fornitore, possono essere scaricate direttamente dal sistema nella smart card, sfruttando la possibilità della stessa di eseguire i programmi scaricati tramite il suo chip, e lo strato di software ad esso associato, qui rappresentati come una macchina virtuale VM.

Il tutto con l'ulteriore possibilità, da parte del fornitore, di controllare e verificare l'effettiva abilitazione di un particolare utente a riceve-

re determinati programmi. E' infatti soltanto a seguito della avvenuta iscrizione di un determinato utente (ad esempio a seguito della sottoscrizione di un abbonamento) all'insieme degli utenti abilitati a ricevere un dato servizio che il fornitore provvede a diffondere l'informazione che, elaborata a livello di smart card 105, consente all'utente stesso di ricevere il servizio.

Da quanto precede risulta altresì evidente che, pur essendo preferita (per motivi meglio spiegati nel seguito) l'attuazione a livello di un supporto mobile quale una smart card, la stessa funzione può essere svolta anche in modo diverso, ad esempio sotto forma di una funzione circuitale compresa nel sistema STB dell'utente.

A differenza delle interfacce CA0 e CA1 descritte in precedenza, che sono intrinsecamente interfacce a livello fisico, la soluzione secondo l'invenzione è suscettibile di essere implementata a livello di programmazione, in particolare mediante una smart card, quale, ad esempio, una cosiddetta Java Card.

I termini "Java" e "Java Card" sono marchi registrati della Sun Microsystems. La relativa descrizione, in particolare per quanto riguarda la defini-



zione di cosiddette API (acronimo per Application Programming Interface) è pubblicamente disponibile, alla data di deposito della presente domanda, presso il sito Internet <http://java.sun.com/products/java-card>.

Sotto questo punto di vista, la soluzione secondo l'invenzione può essere identificata come un nuovo livello di interfaccia, indicato nella figura 2 come CA2 per conformità con le denominazioni CA0 e CA1 utilizzate in precedenza, corrispondente in pratica ad un livello intermedio dell'unità di utente 105. All'atto pratico, la soluzione secondo l'invenzione prevede che il cosiddetto "trusted middleware" previsto dal modello di riferimento OPIMA sia suddiviso in una parte statica TMW1, compresa, secondo la soluzione illustrata nella figura 2, nel modulo STB, ed una parte dinamica TMW2, compresa nell'unità di utente 105.

Il complesso di funzioni rappresentato da TMW1 comprende in particolare un modulo SP' la cui funzione è essenzialmente quella di estrarre un algoritmo specifico del fornitore SP a partire dal flusso di dati MPEG proveniente dal ricevitore 100 (figura 1) per caricarlo nell'unità di utente 105 come parte specifica. Di preferenza tale algoritmo è in-

serito come flusso di dati privati in conformità con lo standard ISO/IEC 13818 già menzionato. La parte rimanente nell'insieme di funzioni TMW1 è costituita dal descrambler 102 e dalle relative funzioni rappresentate dai moduli 101 e 104 nello schema della figura 1. Il complesso di parti e funzioni TMW1 risulta pertanto completamente definito e del tutto indipendente dal fornitore SP di volta in volta coinvolto e di conseguenza è di tipo standardizzato. In pratica, la funzione indicata come TMW2 è identificata da un algoritmo specifico del singolo fornitore SP che viene scaricato nell'unità di utente 105 in modo sicuro (ad esempio in quanto provvisto di firma crittografica) attraverso la funzione SP'.

In questo modo l'algoritmo scaricato è suscettibile di essere eseguito nell'unità di utente 105 in un ambiente sicuro, proprio per le ben note doti di resistenza alla manomissione delle smart card.

Questo spiega il perché, pur essendo in via di principio attuabile anche ricorrendo ad un circuito o ad una funzione incorporata nel sistema STB dell'utente, la soluzione secondo l'invenzione viene realizzata di preferenza a livello di una unità di utente 105 costituita da una smart card. Questa scelta consente anche di sostituire facilmente una

smart card eventualmente danneggiata o alterata.

Nell'impiego, quando l'utilizzatore U sceglie un particolare fornitore SP (ciò può essere fatto tramite una normale operazione di selezione attuata agendo su un telecomando - non illustrato ma associato in modo noto al sistema STB - secondo le normali modalità adottate, ad esempio, per la selezione di un programma televisivo) un cosiddetto applet generato dal fornitore SP in questione viene trasferito verso il sistema STB in vista del caricamento nella rispettiva unità 105. Come noto, per applet si intende un insieme di istruzioni Java che realizza un determinato algoritmo. La diffusione può avvenire, ad esempio, nel caso di trasmissioni diffuse tramite onde radio sfruttando la configurazione a giostra (carousel) adottata per la diffusione dei dati MPEG-2 DSM-CC (acronimi per Digital Storage Media Command Control).

In questo modo, nell'ambito della funzione TMW1 il filtro 101 (figura 1) viene programmato in vista dell'estrazione dei dati EMM, specifici del singolo utente abilitato.

I messaggi EMM possono essere così letti e decifrati in vista dell'interpretazione dei dati contenuti nei messaggi ECM. E' così possibile procedere

all'estrazione della chiave di decifrazione CW relativa al servizio che viene inviata verso il descrambler 102, in modo da consentire la funzione del servizio da parte dell'utente U attraverso il demultiplicatore 106 e il decodificatore 107.

Naturalmente, è anche possibile prevedere funzioni addizionali, quale quella che prevede il trasferimento sicuro verso il fornitore SP di informazioni specifiche relative al servizio erogato, quale ad esempio informazioni inerenti all'entità di consumo del servizio richiesto.

Un esempio specifico di funzionamento secondo i criteri generali appena richiamati è illustrato nel diagramma di flusso della figura 3.

A partire da un passo iniziale 200, il passo indicato con 201 rappresenta la scelta, da parte dell'utilizzatore, di un particolare fornitore SP. Questo passo può essere attuato, ad esempio, sintonizzando - in modo noto - il sistema STB su una certa frequenza.

Come risultato (passo 202) il sistema STB in questione comincia a ricevere dal fornitore SP il flusso di trasporto dei dati, ad esempio nel formato MPEG-2, trasmesso dal fornitore SP.

Il passo 203 rappresenta l'estrazione della



JACOBACCI & PERANI S.p.A.

funzione TMW2 (di tipo dinamico) da parte della funzione SP'.

Dopo aver ripristinato (nel passo 204) l'unità utente 105, nel successivo passo 205 il sistema STB installa nella stessa (ad esempio come applet di Java Card) la funzione TMW2. Il sistema STB richiede poi (passo 206) alla stessa unità 105, in particolare alla parte di macchina virtuale VM che è in grado di elaborare i dati estratti, come inizializzare la funzione di filtro, rappresentata dal blocco 101 nella figura 1.

A questo punto (passo 207) il sistema STB comincia ad inviare verso l'unità di utente 105 i dati EMM filtrati completando così l'abilitazione della comunicazione fornitore/utente. Quest'ultimo può allora scegliere (passo 208) il servizio desiderato. A questo punto il sistema STB comincia a filtrare i segnali ECM associati al servizio prescelto inviandoli verso l'unità di utente 105 dove si verifica (passo 210) se l'utilizzatore è abilitato ad accedere al servizio.

In caso di esito negativo (utente non abilitato), il funzionamento evolve verso un'ulteriore fase di scelta di un eventuale altro servizio (passo 216 di cui si dirà nel seguito).

Se, al contrario, l'utente risulta abilitato (esito positivo del passo di confronto 210) in quanto registrato come tale presso il fornitore SP, in particolare in relazione al servizio prescelto, i dati ECM vengono decifrati dall'unità 105 (passo 211) restituendo le rispettive parole di controllo verso il sistema STB (passo 212).

In questo modo la funzione TMW1 (statica) del sistema STB è in grado di decifrare il servizio portandolo in chiaro (passo 213) in vista dell'erogazione all'utente (passo 214) attraverso i moduli 106 e 107.

Il passo 215 è diretto a verificare se l'utente, con l'applicazione al sistema STB di un ordine (ad esempio impartito tramite telecomando) abbia espresso la volontà di interrompere la fruizione del servizio o se il servizio stesso sia terminato.

Se non è così (esito negativo del passo 215) il funzionamento ritorna a monte del passo 211, con la possibilità di tener conto di un'eventuale periodica variazione della chiave di decifrazione CW.

In caso di esito positivo del passo 215, in un successivo passo 216 si verifica se l'utente sia intenzionato a usufruire di un nuovo servizio. Come già detto, il funzionamento può evolvere verso il

passo 216 anche nel caso di esito negativo del passo 210, così da consentire ad un utente non abilitato alla fruizione di un determinato servizio di scegliere un servizio diverso.

L'esito negativo del passo 216 determina l'evoluzione verso una fase terminale 300. Si apprezzerà che questa non corrisponde di solito ad un vero e proprio arresto del sistema STB ma soltanto al raggiungimento di uno stato di attesa (idle).

L'esito positivo del passo 216 determina il ritorno verso il passo 201 di scelta di un nuovo fornitore ovvero verso il passo 208 di scelta di un nuovo servizio erogato dallo stesso fornitore utilizzato in precedenza a seguito dell'esito di un corrispondente passo di scelta 217.

Naturalmente, fermo restando il principio dell'invenzione, i particolari di realizzazione e le forme di attuazione potranno essere ampiamente variati rispetto a quanto descritto ed illustrato, senza per questo uscire dall'ambito della presente invenzione, così come definita dalle rivendicazioni annesse.

RIVENDICAZIONI

1. Procedimento per l'erogazione controllata di servizi numerici nell'ambito di una pluralità di fornitori (SP) ed utenti (U), in cui detti servizi sono identificati da rispettivi flussi di dati codificati erogati da detti fornitori (SP) e gli utenti sono provvisti di mezzi di ricezione (STB) per ricevere detti flussi di dati, i mezzi di ricezione essendo selettivamente abilitati alla fruizione di servizi determinati attraverso una rispettiva unità di utente (105), caratterizzato dal fatto che comprende le operazioni di:

- incorporare in detti flussi di dati codificati almeno un algoritmo di abilitazione alla fruizione di rispettivi servizi determinati (TMW2),

- incorporare in detti flussi di dati codificati un rispettivo codice identificativo (EMM) per ciascun utente (U) da abilitare alla ricezione di un determinato servizio,

- associare a detta unità d'utente (105) una funzione elaborativa (VM) suscettibile di riconoscere ed eseguire detto almeno un algoritmo di abilitazione sulla base di detto codice identificativo per abilitare i mezzi di ricezione (STB) del rispettivo utente alla fruizione di detto servizio.

JACOBACCI & PERANI S.p.A.



2. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che comprende l'operazione di configurare detta unità di utente (105) quale supporto elaborativo mobile assegnato univocamente ad uno di detti utenti (1) ed associabile selettivamente a detti mezzi di ricezione (STB), detti mezzi di ricezione (STB) essendo di tipo generalizzato comune a più utenti di detta pluralità (U).

3. Procedimento secondo la rivendicazione 2, caratterizzato dal fatto che comprende l'operazione di configurare detto supporto elaborativo mobile come smart card.

4. Procedimento secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto che comprende le operazioni di:

- associare a detti mezzi di ricezione (STB) una funzione di trusted middleware (TMW),

- configurare detta funzione di trusted middleware in una parte statica (TMW1), residente su detti mezzi di ricezione (STB), ed in una parte dinamica (TMW2) selettivamente trasferibile su detta unità di utente (105) in vista dell'esecuzione di detto almeno un algoritmo da parte di detta funzione elaborativa (VM).

5. Procedimento secondo una qualsiasi delle prece-

denti rivendicazioni, caratterizzato dal fatto che comprende le operazioni di:

- configurare detti flussi di dati come flussi di dati di tipo MPEG contenenti messaggi di tipo EMM,

- inserire detto codice identificativo nei messaggi di tipo EMM,

- attivare, tramite detta unità di utente (105), a seguito della ricezione di detto almeno un algoritmo, lo svolgimento delle seguenti funzioni:

- estrazione, lettura e decifrazione dei messaggi EMM contenuti nel flusso di dati ricevuto,

- interpretazione di detto codice identificativo contenuto nei messaggi EMM,

- esecuzione di detto almeno un algoritmo di abilitazione sulla base di detto codice identificativo.

6. Procedimento secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto che detto almeno un algoritmo di abilitazione viene incorporato in un flusso di dati privati nell'ambito di detti flussi di dati.

7. Procedimento secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto che a

seguito della ricezione di detto almeno un algoritmo, detta funzione elaborativa (VM) abilita detti mezzi di ricezione per il funzionamento quali trasmettitori per emettere informazioni relative all'erogazione del servizio stesso.

8. Sistema per l'erogazione controllata di servizi numerici nell'ambito di una pluralità di fornitori (SP) ed utenti (U) in cui detti servizi sono identificati da rispettivi flussi di dati codificati erogati da detti fornitori (SP) e gli utenti sono provvisti di mezzi di ricezione (STB) per ricevere detti flussi di dati, i mezzi di ricezione essendo selettivamente abilitati alla fruizione di servizi determinati attraverso una rispettiva unità di utente (105), caratterizzato dal fatto che:

- detti fornitori (SP) sono configurati per incorporare nei rispettivi flussi di dati codificati, almeno un algoritmo di abilitazione alla fruizione di rispettivi servizi determinati, nonché per incorporare in detti flussi di dati codificati, un rispettivo codice identificativo (TMW2), per ciascun utente (U) da abilitare alla ricezione di un determinato servizio,

- dette unità d'utente (105) portano associata una funzione elaborativa (VM) suscettibile di rico-

noscere ed eseguire detto almeno un algoritmo sulla base di detto codice identificativo per abilitare i rispettivi mezzi di ricezione (STB) del rispettivo utente alla fruizione di detto servizio.

9. Sistema secondo la rivendicazione 8, caratterizzato dal fatto che dette unità di utente (105) sono configurate quali supporti elaborativi mobili assegnati univocamente ciascuno ad uno di detti utenti (1) ed associabili selettivamente a detti mezzi di ricezione, detti mezzi di ricezione essendo di tipo generalizzato comune a più utenti di detta pluralità (U).

10. Sistema secondo la rivendicazione 9, caratterizzato dal fatto che detti supporti elaborativi mobili sono configurati come smart card.

11. Sistema secondo una qualsiasi delle precedenti rivendicazioni 8 a 10, caratterizzato dal fatto che

- detti mezzi di ricezione (STB) portano associata una funzione di trusted middleware (TMW) configurata in una parte statica (TMW1), residente su detti mezzi di ricezione (STB), ed in una parte dinamica (TMW2) selettivamente trasferibile sulla rispettiva unità di utente (105) in vista dell'esecuzione di detto almeno un algoritmo da parte di detta funzione elaborativa (VM).



13. Sistema secondo una qualsiasi delle precedenti rivendicazioni 8 a 11, caratterizzato dal fatto che detti fornitori di servizi erogano detti flussi di dati come flussi di dati di tipo MPEG contenenti messaggi di tipo EMM con detto codice identificativo inserito in detti messaggi di tipo EMM, e detti mezzi di ricezione comprendono:

- mezzi di estrazione, lettura e decifrazione dei messaggi EMM contenuti nel flusso di dati ricevuto,
- mezzi di interpretazione (103, 104) per interpretare detto codice identificativo contenuto nei messaggi EMM, e
- mezzi elaborativi (VM) per eseguire detto almeno un algoritmo di abilitazione sulla base di detto codice identificativo.

13. Sistema secondo una qualsiasi delle precedenti rivendicazioni 8 a 12, caratterizzato dal fatto che detti fornitori di servizi incorporano detto almeno un algoritmo di abilitazione in un flusso di dati privati nell'ambito di detti flussi di dati.

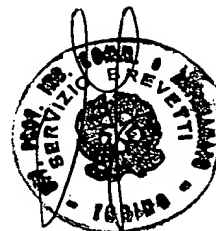
14. Sistema secondo la rivendicazione 13, caratterizzato dal fatto che i mezzi di ricezione sono attivabili da detta unità di utente (105) a seguito della ricezione di detto almeno un algoritmo per il

funzionamento quali trasmettitori per emettere informazioni relative all'erogazione del servizio stesso.

15. Sistema secondo una qualsiasi delle rivendicazioni 8 a 14, caratterizzato dal fatto che detta unità di utente (105) è configurata come Java Card.

PER INCARICO

Ing. Paolo CIAN
N. 1000 505
[il progetto è per gli altri]



JACOBACCI & PERANI S.p.A.

